Πανεπιστήμιο Πελοποννήσου
Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πρόγραμμα Μεταπτυχιακών Σπουδών στην
Επιστήμη και Τεχνολογία των Υπολογιστών

Θέματα Δικτυοκεντρικού Προγραμματισμού

Penetration Testing

Γκούντης Θοδωρής
ΑΜ: 2022201520005
E-Mail: thodorisgudis@gmail.com

Διδάσκων
Αναπλ. Καθηγητής Κ. Βασιλάκης

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Ως δοκιμή διείσδυσης (αγγλ.: penetration testing, ή αλλιώς pentest) ορίζεται μια δοκιμαστική εισβολή σε ένα πληροφοριακό σύστημα για την αξιολόγηση της ασφάλειας του. Με την μέθοδο αυτή γίνεται μια προσομοίωση μιας επίθεσης από κακόβουλο εισβολέα που έχει σκοπό την εκμετάλλευση κενών ασφαλείας για την ανάδειξη των ευπαθειών του συστήματος.

Το Penetration Testing ή κατά το ελληνικό “Δοκιμές Διείσδυσης” αποτελεί ένα από τα εργαλεία ανίχνευσης των αδυναμιών ασφάλειας πληροφοριών, το οποίο προχωρά ένα βήμα παραπάνω καθώς εκμεταλλεύεται την κάθε αδυναμία, με σκοπό να διεισδύσει στα πληροφορικά συστήματα.

Η αξία του Penetration Testing ως μεθόδου ανίχνευσης αδυναμιών ασφάλειας έχει τεθεί πολλές φορές υπό αμφισβήτηση, ειδικά από Οργανισμούς οι οποίοι θεωρούν ότι έχουν διαμορφώσει ένα ικανοποιητικό επίπεδο ασφάλειας πληροφοριών. Τι είναι όμως το Penetration Testing και ποιους συγκεκριμένους τύπους διακρίνουμε;

Στη πιο απλή του μορφή το PenTest αποτελεί ανεξάρτητο έλεγχο του επιπέδου ασφάλειας πληροφοριών ενός Οργανισμού, κάνοντας χρήση τεχνικών οι οποίες προσομοιώνουν επιθέσεις από κακόβουλους χρήστες (είτε αυτοί βρίσκονται στο εσωτερικό του Οργανισμού είτε προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση μέσω των διασυνδέσεών του με το διαδίκτυο και τις λοιπές διασυνδέσεις του Οργανισμού).

1.1 ΧΑΚΕΡ

Χάκερ (Hacker) ονομάζεται το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ένας χάκερ έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα.

Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες αποκαλούνται κράκερ

1.2 HACKING VS ETHICAL HACKING

Αν και ουσιαστικά και οι δυο κατηγορείς έχουν καλή γνωστή των δικτυών και των υπολογιστικών Συστημάτων και χρησιμοποιούν και τα ιδιά εργαλεία και τις ιδιες μεθόδους. Υπάρχει μια Σημαντική Διάφορα αυτό που τους ξεχωρίσει . Η διάφορα είναι **η Άδεια (permission).** Ο ethical hacker συνήθως είναι ειδικός σε θέματα ασφάλεια πληροφορικών συστημάτων και το σημαντικότερο είχε άδεια και πολλές φορές του ζητάτε μάλιστα να δοκιμάσει τα σύστημα ενός οργανισμού ή μιας επιχείρησης έναντι πιθανόν κακοβουλιών ή μη επιθέσεων από αλλους Χακερ.

1.3 ΟΙ ΤΥΠΟΙ ΤΩΝ HACKER

Αν και είναι δύσκολο να κατηγοριοποιήσεις τους Χακερ, εδώ θα τους κατηγοριοποιήσουμε με βάση τον τρόπο και τον σκοπό που χρησιμοποιούν τις ικανότητες τους και είναι και πιο κοντά και στο θέμα της εργασίας μας.

Με βάση αυτή την Κατηγοριοποιήσει έχουμε τους:

- **Black Hat Hacker ή cracker**. Άτομα με υψηλή ειδίκευση στους υπολογιστές, χρησιμοποιούν τις δεξιότητές τους με μη ηθικούς τρόπους
- **Grey Hat Hacker**, χαρακτηρίστηκαν και ως «hacktιβιστές (hacktivists)», δηλαδή τα άτομα που χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να μεταφέρουν πολιτικά μηνύματα.
- **White Hat Hacker, (penetration) ή hacker.** Χρησιμοποιούν την ικανότητά τους σαφώς κατά ηθικό τρόπο. Είναι παραδείγματος χάρη, οι υπάλληλοι εταιρειών, οι οποίοι έχουν άδεια να επιτίθενται στα δίκτυο και τα συστήματα της εταιρείας τους για τον καθορισμό των αδυναμιών

1.4 ΣΗΜΑΝΤΙΚΟΙ ΟΡΙΣΜΟΙ

Πριν ξεκινήσουμε να μιλήσουμε για το Penetration Testing θα δούμε πρώτα κάποιους σημαντικούς ορισμούς, που θα τους συναντήσουμε πολύ συχνά και την σημασία τους

- **Asset (Περιουσιακό Στοιχείο ή Κεφάλαιο)**. Το asset είναι αυτό που προσπαθούμε να προστατεύσουμε Άνθρωποι, Ιδιοκτησία και Πληροφορίες
- **Vulnerability (Ευπάθεια ή τρωτό σημείο).** Μια αδυναμία ή ένα κενό στην ασφάλεια ενός συστήματος ή προγράμματος που μπορεί να αξιοποιηθεί για να έχουμε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα asset.
- ***Vulnerability is the birthplace of innovation, creativity and change. (Brene Brown)***
- **The Threat (Απειλή).** Η Απειλή είναι αυτό από το οποίο θέλουμε να προστατευτούμε Οτιδήποτε και οποιοσδήποτε που μπορεί να εκμεταλλευτεί την ευπάθεια , εκούσια ή τυχαία και να αποκτήσουν πρόσβαση ή να προκαλέσει βλάβη , ή να καταστρέψει ένα περιουσιακό στοιχείο (asset)
- **EXPLOIT (ΑΞΙΟΠΟΙΗΣΗ, ΕΚΜΕΤΑΛΛΕΥΣΗ)**. Η αξιοποίηση είναι η χρήση των τρωτών σημείων του συστήματος με σκοπό να προκαλέσουμε ακούσιες ή απρόβλεπτες συμπεριφορές σε ενα σύστημα, το οποίο έχει σαν στόχο να επιτρέψει στον επιτιθέμενο να αποκτήσει πρόσβαση σε δεδομένα και πληροφορίες.
- **RISK (ΚΙΝΔΥΝΟΣ)** Η πιθανότητα για την απώλεια , φθορά ή καταστροφή ενός περιουσιακού στοιχείου (asset), ως αποτέλεσμα της απειλής που εκμεταλλεύεται μια ευπάθεια.

  Μπορούμε να την υπολογίσουμε με την συνάρτηση.

Risk = Threats * Vulnerabilities * Impact(Επιπτώσεις)

2. PENETRATION TESTING

Ο στόχος του Penetration Testing είναι να απεικονίζουμε το τρέχον επίπεδο ασφάλειας της εταιρείας και ο εντοπισμός των κενών, τόσο των υπολογιστικών συστημάτων όσο και του ανθρώπινου δυναμικού έναντι των πιθανών παραβιάσεων.

Δηλαδή προσπαθούμε να ανακαλύπτουμε, τι όγκος από ευαίσθητες πληροφορίες θα χαθούν σε περίπτωση επίθεσης. Επίσης Θέλουμε να δοκιμάσουμε την Ομάδα Ασφαλείας μας και τους Διαχειριστές Δικτύων.

Άλλος ενας λογος να Θέλουμε να δοκιμάσετε μια νέα υπηρεσία ή ένα σύστημα , πριν αυτή βρεθεί online και Θέλουμε να μάθουμε τα τρωτά σημεία των δικτύων , των συστημάτων και των εφαρμογών σας πριν αυτή αρχίσει να τρέχει και βρεθούμε εκτεθειμένη.

Γιατί να θέλουμε να μπούμε σε μια τέτοια χρονοβόρα και κοστοφορα διαδικασία;

Οι Αναφορές από Ανεξάρτητα Ινστιτούτα για IT-Security αναφέρουν ότι 150,000 malware κατασκευάστηκαν το 2014. Το Ινστιτούτο AV-TEST ανέφερε ότι 390,00 νέα malwares ανακαλύπτονται κάθε μέρα. Οι αναφορές από το Kaspersky LAB αναφέρουν ότι για το 2014 βρέθηκαν 6,167,233,068 malwares και αναφέρθηκαν 1,432,660,467 επιθέσεις σε κινητά.

Επίσης οι μισές εταιρίες που εμπλέκονται στο E-Business έχουν υποστεί ζημιά λόγω επιθέσεων. Πιο συγκεκριμένα οι Carbanak, μια συμμορία του κυβερνοχώρου με οικονομικά κίνητρα έχει καταφέρει να κλέψει 1 δις δολαρίων ΗΠΑ (με τη χρήση κακόβουλου λογισμικού και εξ αποστάσεως) σε 30 διαφορετικές χώρες . Η Sony έχει δεκτή επίθεση στο δίκτυο του playstasion, η οποία προκάλεσε μια μεγάλη απώλεια στην φήμη από την εταιρεία και τέλος στην HSBC Turkey το Νοεμβρίου 2014 κλάπηκαν Πληροφορίες από 2.700.000 πιστωτικές κάρτες και αυτές είναι μόνο κάποιες υποθέσεις που γίνονται γνωστές, αν αναλογιστούμε ότι κάθε μέρα ανακαλύπτουμε διαφορετικές τύπους επιθέσεων και μεθόδων μπορούμε να αντιληφθούμε την ανάγκη υπάρξεις μια τέτοια διαδικασίας.

2.1 ΤΑ ΟΦΕΙΛΕΙ ΤΟΥ PENTEST?

Όπως αναφέρομαι και πιο πάνω κατά την εκτέλεση ενός penetration testing οι αδυναμίες ενός συστήματος εκτίθενται διευκολύνοντας έτσι την ανάλυση των πραγματικών κινδύνων.

Επίσης Βοηθά στη διατήρηση της επιχειρησιακής συνέχειας – συνεχή και απρόσκοπτη λειτουργία του συστήματος μας. Προστατεύει το προσωπικό , τους πελάτες και τις επιχειρήσεις. Μειώνει τις πιθανότητες για πραγματική επιθέσεις και Αυξάνει την τεχνογνωσία και διευκολύνει την ανάλυση για την πραγματική επιθέσεις.

Άλλο ένα σημαντικοί χαρακτηριστικοί είναι ότι προστατεύει την φήμη της Εταιρεία μας και Τέλος Βοηθά να συμμορφώνεται η εταιρεία με πιστοποιήσεις όπως ISO27001 και PCI DSS που πιθανόν να χρειάζεται για να τρέξει κάποιες υπηρεσίες.

2.2 ΠΩΣ ΠΡΑΓΜΑΤΟΠΟΙΕΙΤΑΙ ΕΝΑ PENTEST?

Αρχικά ορίζουμε τον Στόχο και τον Σκοπό του Τεστ ο οποίος μπορεί να είναι:

- Web app pentest
- End user and social engineering attacks
- Ddos and performance tests
- Networwork infracture tests
- External and internal network tests
- Mobile app pentest
- Virtualization system pentest
- Database pentest

ΤΑ ΣΤΑΔΙΑ ΕΚΤΕΛΕΣΕΙΣ ΤΟΥ TEST

- Συλλογή πληροφοριών -(Information gathering)
- Ανάλυση και Σχεδιασμός - (Analysis and plan)
- Ανακαλύπτουμε τα Τρωτά Σημεία -(Discover vulnerabilitites)
- Εξερεύνηση -(Exploration)
- Αποκτάμε Πρόσβαση - (Gaining Access)
- Αναφορά (Privilege and Reporting)
- Ελέγχουμε αν έχει Επιδιορθωθεί - (Post-Fix Verification)

ΣΤΟΧΟΣ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ ΜΕ ΤΟ PENTEST

Οι παρακάτω τομείς ελέγχονται ενάντια σε πιθανές αδυναμίες ή δυσλειτουργίες του συστήματος.

- Mistakes/Shortcomings in application develoment
- Configuration errors
- Security awareness of staff
- System protection level
- Insecure certificate usage
- Patch level of Applications
- Patch level of Operating Systems

Ελέγχονται έτσι ώστε να εντοπιστεί το επίπεδο ασφάλειας του συστήματος μας.

2.3 ΚΑΝΟΝΕΣ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

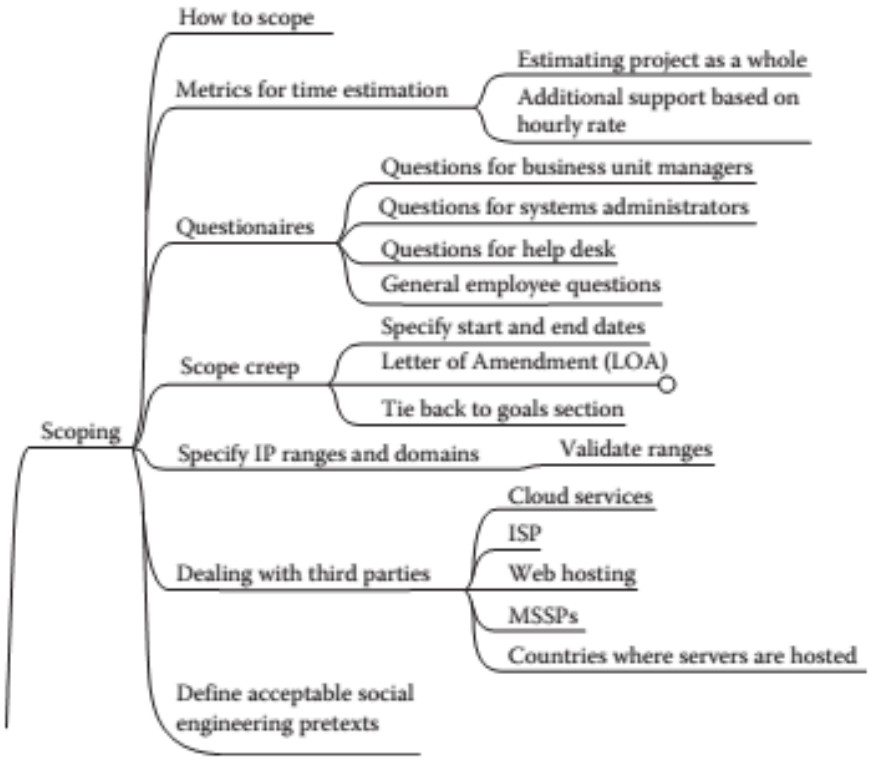
Πριν ξεκινήσουμε οτιδήποτε ορίζουμε με τους πελάτες μας τις ενέργειες που μας επιτρέπονται να κάνουμε και τους κανόνες που θα ακολουθήσουμε κατά την διάρκεια της δοκιμής μας.

Πιο συγκεκριμένα ορίζουμε:

- Το πως θα πραγματοποιηθεί η διαδικασία αναλυτικά.
- Ποιες μεθόδους Θα χρησιμοποιήσουμε.
- Την ημερομηνία Έναρξης και Λήξης της δοκιμής.
- Τα ορόσημα, και της σημαντικές Ημερομηνίες
- Το σκοπό του Test
- Οι επιτρεπόμενες και μη τεχνικές. Παράδειγμα εάν θα τρέξουμε κάποια επίθεση DDoS
- Τις υποχρεώσεις και τις ευθύνες κάθε μέλους

Αυτά πρέπει να συμφωνηθούν αμοιβαία τόσο από τον πελάτη όσο και από τον tester, πριν ακόμα ξεκινήσει η διαδικασία και ακολουθούνται κατά γράμμα.

(http://www.pentest-standard.org/index.php/Pre-engagement)



ΟΡΟΣΗΜΑ – ΣΗΜΑΝΤΙΚΕΣ ΗΜΕΡΟΜΗΝΙΕΣ

Κάλο είναι πριν ξεκινήσουμε το τεστ να έχουμε ορίσει ένα χρονοδιάγραμμα εργασιών. Που θα περιλαμβάνει τις ενέργειες που πραγματοποιούμε, το χρονικό διάστημα που τις πραγματοποιούμε και την φάση που βρισκόμαστε ως προς την εκτέλεση της διαδικασίας. Υπάρχουν αρκετά εργαλεία χρόνο προγραμματισμού στο διαδίκτυο ή και διαδικτυακές εφαρμογές όπως το Bacecamp (https://basecamp.com/) ή μπορούμε να χρησιμοποιήσουμε ακόμα και ένα απλό Excel για να κάνουμε την δουλειά μας.

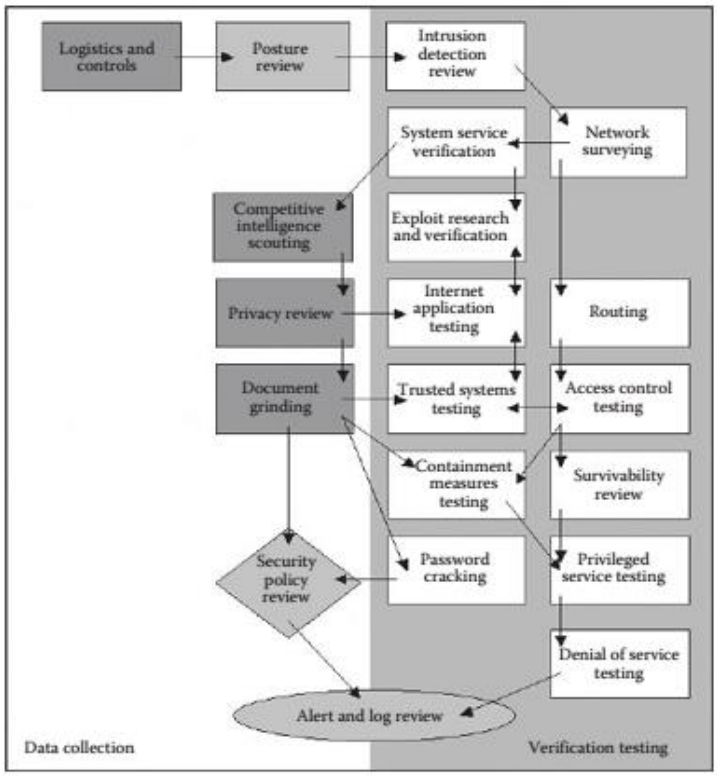
Start	End	Month	Year	Phases
12th May 2013	18th	May	2013	Scope Definition
19th May 2013	27th	May	2013	Reconnaisance
28th May 2013	2th	June	2013	Scanning
3rd june 2013	16th	june	2013	Exploitation
17th June 2013	21th	June	2013	POST Exploitation
21st June 2013	28th	June	2013	Reporting

2.4 PENETRATION TESTING METHODOLOGIES

Σε κάθε τεστ η μεθοδολογία και η αναφορά είναι το πιο κρίσιμο κομμάτι. Υπάρχουν αρκετές διαφορετικές μεθοδολογίες που μπορούμε να ακολουθήσουμε για το πως να υλοποιήσουμε την δοκιμή μας. Εδώ θα δούμε τρεις από αυτές και τα χαρακτηριστικά τους.

OOSTMM

Το OOSTMM (open source security testing methology) συμπεριλαμβάνει όλα τα βήματα που περιλαμβάνονται σε ένα τεστ, πράγμα που την κάνει χρονοβόρα, κουραστική, ακριβή και δύσκολο να εφαρμοστή σε καθημερινή βάση.



NIST

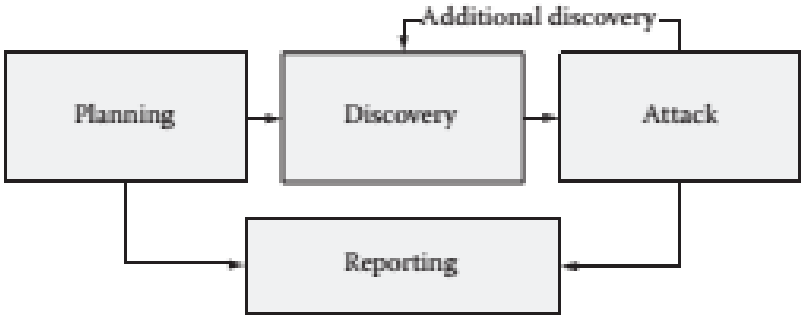
Είναι πιο σύντομη από την προηγουμένη και μπορεί να εφαρμοστή σε καθημερινή βάση.

Αποτελείται από τέσσερις φάσης:

1. Planning – Σχεδιάζουμε το πως θα εκτελεστεί τη δοκιμή.
2. Discovery

   Βήμα 1 -Συλλογή πληροφοριών, σκαναρισμα του δικτύου, αναγνώριση υπηρεσιών και OS

   Βήμα 2 – Εκτίμηση Αδυναμιών
3. Attack, επίθεση στον στόχο
4. Report, καταγράφουμε την αντίδραση του στόχου



OWASP(OPEN WEB APPLICATION SECURITY PROJECT)

Είναι σχεδιασμένη για application penetration test. Περιέχει σχεδόν οτιδήποτε θα χρειαστείς για να δοκιμάσεις μια διαδικτυακή πλατφόρμα. Η μεθοδολογία αυτή είναι πλήρης και έχει σχεδιαστεί από ειδικούς στην ασφάλεια διαδικτυακών εφαρμογών

2.5 ΚΑΤΗΓΟΡΙΕΣ PENETRATION TEST

- **Black Box,** δεν γνωρίζουμε τίποτα για τον στόχο μας, συνηθισμένο σε εξωτερικό penetration test.
    - Network penetration, δεν γνωρίζουμε το OS, έκδοσή server κ.α
    - Web application – δεν έχουμε το κώδικά της διαδικτυακής υπηρεσίας
- **White Box,** ξέρουμε τα πάντα σχετικά με τον στόχο μας, συνήθως σε εσωτερικό penetration test.
    - Network penetration, εφαρμογές που τρέχουν, το OS, έκδοσή server κ.α
    - Web application – μας παρέχετε ο κώδικά της διαδικτυακής υπηρεσίας
- **Gray Box,** έχουμε κάποιες πληροφορίες και κάποιες όχι.
    - Network penetration, ξέρουμε τις εφαρμογές που τρέχουν άλλα όχι την έκδοση τους
    - Web application – μας παρέχετε κάποιες πληροφορίες πχ, ένα test account, εναν back end server και πιθανόν κάποια βάση

2.6 ΤΥΠΟΙ PENETRATION TESTING

- **Network Pentest** Δοκιμάζουμε το περιβάλλον ενός δικτύου για πιθανά τρωτά σημεία και απειλές το οποίο χωρίζεται σε εξωτερικός έλεγχος (π.χ public ip addresses) και εσωτερικός έλεγχος(p.x vpn)
- **Web Application Pentest.** Είναι ο πιο κοινός έλεγχος που κάνουμε καθώς στις web apps έχουμε πολλές κρίσιμες πληροφορίες(πιστωτικές κάρτες, κωδικούς πρόσβασης, ονόματα χρηστών).
- **Mobile Application Pentest.** Το νεότερο είδος ελέγχου καθώς τα κινητά με android και iOS παρέχουν υπηρεσίες στους χρήστες τους και για κάποιους αποτελούν στόχο
- **Wireless Pentest.** Προσπαθούμε να έχουμε πρόσβαση σε ασύρματα δίκτυα
- **Social Engineering Pentest.** Μπορεί να είναι και μέρος ενός web application test και Μπορεί να επιτεθείς στους χρήστες του κοινωνικοί δικτύου μεσώ τεχνικών phishing, browser exploits με σκοπό να ξεγελάσεις τον χρήστη και να κάνει ενέργειες που δεν θέλει να κάνει
- **Physical Pentest.** Είναι το πιο σπάνιο και περιλαμβάνει πχ έλεγχο κλειδαριών και μηχανισμών RFID.

3. ΕΓΓΡΑΦΗ ΤΗΣ ΑΝΑΦΟΡΑΣ - REPORT WRITING

Η αναφορά είναι το πιο κρίσιμο σημείο σε ένα penetration test. Για αυτό Θα πρέπει να είναι: **Απλή, Ξεκάθαρη και Κατανοητή .** Η παρουσίαση της είναι επίσης σημαντική (π.χ καλή μορφοποίηση και σωστή χρήστη χρωμάτων, γραμματοσειρών).

Να είναι καλά οργανωμένη, σωστή σύνταξη και Ορθογραφία. Γράψουμε στο στυλ και στο είδος την αναφοράς. Προσπαθούμε να μειώσουμε πιθανές Αστοχίες. Κάνουμε μια λεπτομερής αναφορά των τρωτών σημείων που βρήκαμε, ένα στιγμιότυπο της οθόνης θα ήταν πολλή χρήσιμο και αποτελεσματικό.

3.1 ΤΟ ΚΟΙΝΟ ΤΗΣ ΑΝΑΦΟΡΑΣ ΜΑΣ

Έχουμε χωρίσει το κοινό σε τρεις κατηγορίες

1. **Διευθύνων Σύμβουλος (CEO),** Ενδιαφέρεται κυρίως για μια εκτελεστική αναφορά , την αναφορά αποκατάστασης
2. **Ο διευθυντής του τμήματος,** που πιθανόν να είναι υπεύθυνος και για την ασφάλεια Πιθανόν θα θέλουν να δουν τις συνολικές αδυναμίες άλλα και δυνατά σημεία, την αναφορά αποκατάστασης, την εκτίμηση αδυναμίας κ.α
3. **Οι Τεχνικοί,** Θα εξετάσουν την αναφορά αναλυτικά, καθώς είναι υπεύθυνη για να διορθώσουν τις αδυναμίες και να σιγουρευτούν ότι έχουν διορθώσει τα κενά ασφάλεια

3.2 ΔΟΜΗ ΤΗΣ ΑΝΑΦΟΡΑΣ ΤΟΥ PENETRATION TEST

ΕΞΩΦΥΛΛΟ - COVER PAGE

Φροντίζουμε να περιέχει το λογότυπο της εταιρίας μας, τον τίτλο και μια περιγραφή για το τεστ. Είναι το πρώτο που βλέπει κάποιος άρα θέλουμε να κάνει καλή εντύπωση

ΠΕΡΙΕΧΟΜΕΝΑ

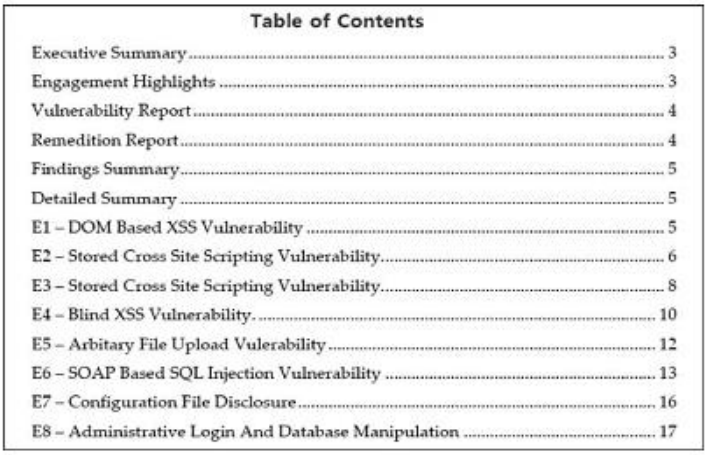
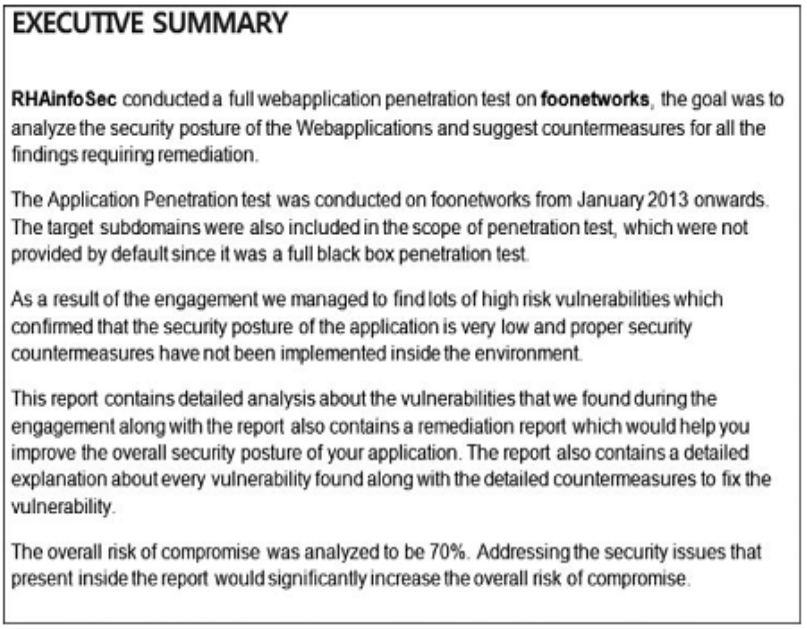


Table of Contents

EXECUTIVE SUMMARY

Είναι σχεδιασμένο να διαβαστεί από μη τεχνικό προσωπικού. Γι' αυτό πρέπει :

- Να είναι συγκεκριμένο στο θέμα, που μας ζητήθηκε να αναλύσουμε.
- Να ορίζει τον σκοπό του και πως το υλοποιήθηκε η διαδικασία.
- Να αναφέρει τα αποτελέσματα του τεστ με τρόπο κατανοητή για κάθε ενδιαφερόμενο.
- Αναφερόμενου την συνολική αδυναμία του συστήματος και τι προκάλεσε το πρόβλημα.
- Στην συνεχεία αναφέρουμε τον πιθανό κίνδυνο που διατρέχει το σύστημα μας
- Τέλος αναφέρουμε την έκταση του κίνδυνου και το πόσο θα μειωθεί εάν διορθώσουμε τα πρόβλημα που ανακαλύψαμε



EXECUTIVE SUMMARY

RHAinfoSec conducted a full webapplication penetration test on **foonetworks**, the goal was to analyze the security posture of the Webapplications and suggest countermeasures for all the findings requiring remediation.

The Application Penetration test was conducted on foonetworks from January 2013 onwards. The target subdomains were also included in the scope of penetration test, which were not provided by default since it was a full black box penetration test.

As a result of the engagement we managed to find lots of high risk vulnerabilities which confirmed that the security posture of the application is very low and proper security countermeasures have not been implemented inside the environment.

This report contains detailed analysis about the vulnerabilities that we found during the engagement along with the report also contains a remediation report which would help you improve the overall security posture of your application. The report also contains a detailed explanation about every vulnerability found along with the detailed countermeasures to fix the vulnerability.

The overall risk of compromise was analyzed to be 70%. Addressing the security issues that present inside the report would significantly increase the overall risk of compromise.

ΑΝΑΦΟΡΑ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

Αναφέρουμε τις συνολικές μας σύστασής, που μόλις υλοποιηθούν θα διορθώσουν το πρόβλημα. Επειδή αναφερόμαστε πάλι συνήθως σε μη τεχνικούς η αναφοράς μας πρέπει να είναι ακριβής και εύκολη στην κατανόησή τους. Αναφέρουμε τα ευρήματα μας από την εργασία μας. Τέλος αναφέρουμε την συνολική αδυναμία και τα δυνατά σημεία στο σύστημα μας. Εδώ μπορούμε να χρησιμοποιήσουμε εικόνες, διαγράμματα, πίνακες έτσι ώστε να κάνουμε καλύτερα κατανοητά τα αποτελέσματα μας.

REMEDIATION

The security control environment for foonetworks was found very poor, as a result of which there are certain security countermeasures we would like to suggest. With the goal of protecting the Web application's infrastructure, we would recommend you to perform the following actions.

- A perfect plan for fixing the Critical, High, Medium, low risk vulnerabilities should designed and implemented. The vulnerabilities should be fixed in the descending order of priority.
- Secure development life cycle (SDLC) for developing web applications shall be implemented.
- A Web Application Firewall shall be implemented to detect, filter and block all the malicious packets.
- Security Audits shall be performed on the regular basis.
- Early security checks should be performed in the development process.

ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ

Είναι το αναλυτικό μας κομμάτι της αναφοράς Είναι κρίσιμο για τον πελάτη μας καθώς εδώ μπορεί να δει την ένταση του πιθανού κίνδυνου.

Hazard risk assessment matrix

Frequency of Occurrence	Hazard Categories 1 Catastrophic	2 Critical	3 Serious	4 Minor
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Unacceptable High Medium Low

(From http://www.sms-ink.com.)

ΛΕΠΤΟΜΕΡΗ ΑΝΑΦΟΡΑ

Αναφερόμαστε καθαρά στο τεχνικό τμήμα στον security manager και στους developers. Αρα σε αυτό το τμήμα μπορούμε να κάνουμε μια πιο λεπτομερή τεχνική αναφορά που:

Περιγράφουμε την αδυναμία και κάνουμε μια πιο λεπτομερή ανάλυση της

- Πως ανακαλύψαμε την αδυναμία.
- Την πηγή της αδυναμίας.
- Τον πιθανό κίνδυνο που μπορεί να προκύψει
- Και τις απαραίτητες δράσεις για την αποκατάσταση της

DOM Based Cross Site Scripting Vulnerability

Affected Hosts: foonetworks.com

Risk: Critical

Description: A DOM Based XSS is a type of Cross site scripting vulnerability which occurs when the user supplied input passed through a source is not filtered/escaped before it's passed through a vulnerable sink.

Explanation: A dynamic file is being included which handles "location.hash" on the document object model (DOM).

http://foonetworks.com/engine.js

The following lines indicate the vulnerable code:

Lines: 410 – 411:

```
if(t!=undefined){window.location.hash=t;}});
$(window).bind("load",function()
{if(window.location.hash){var _9=window.location.hash.substring(1);}
```

Risk

Since javacsript can access the DOM, an attacker can craft a special piece of javascript that would be able to steal the authentication cookies and send it the domain that he controls. In case of a DOM based XSS, the payload is always executed on the client side, this means this makes it difficult to trace the attacker from the forensics perspective, since the attack vector would not appear inside the log file.

Recommendations:

Any user-generated input should be HTML-encoded at any point where it is copied into application responses.

All HTML metacharacters should be replaced with the corresponding HTML entities.

4. ΕΡΓΑΛΕΙΑ ΓΙΑ ΤΗΝ ΔΟΥΛΕΙΑ

Σε αυτή την ενότητα θα δούμε κάποια εργαλεία που εχουμε στην διάθεση μας για να τρέξουμε το τεστ μας. Υπάρχουν και αλλά εργαλεία αλλά εμείς θα δούμε τα ποιο βασικά και θα τα δούμε περιληπτικά καθώς η λεπτομερή αναφορά τους και επιδηξη τους απαιτεί για κάθε ένα από αυτά άλλη μια εργασία από μονή του αλλά και δεν είναι και ο σκοπός αυτής της εργασία.

4.1 KALI LINUX

Σε αυτή την εργασία χρησιμοποιήσαμε το Kali σαν λειτουργικό σύστημα, μεσά από μια εικονική Μηχανή, για να τρέξουμε το τεστ μας. Πολλά από τα εργαλεία που θα δούμε παρακάτω είναι ήδη προεγκατεστημενα στο Kali. Το Kali Linux είναι μια τροποποιημένη διανομή του Debian Linux και ανήκει στην οικογένεια του UNIX OS. Συντηρείται και χρηματοδοτείται από την Offensive Security Limited (www.offensive-security.com).

Σχεδιαστικέ σαν βασικό στόχο το Penetration Testing και την Ψηφιακή Εγκληματολογία (Digital Forensics) και αναπτύχθηκε από τον Mati Aharoni και τον Devon Kearns από το Offensive Security. Ουσιαστικά αποτελεί μια Επανεγγραφή του Backtrack τον προκάτοχος του Kali Linux. Το BackTrack έχει μια μακρά περίοδο για πάνω από 7 χρονιά σαν η καλύτερη επιλογή από τους pentesters και τους hackers.

Το BackTrack είναι ένα προσαρμοσμένο περιβάλλον ενός λειτουργικού συστήματος προσανατολισμένο στο penetration και μέχρι το 2011 είχε χρησιμοποιηθεί από πάνω από 4 εκατομμύρια ερασιτέχνες και επαγγελματίες ερευνητές Ασφαλείας. Η τελευταία έκδοση, BackTrack 5, βασίζεται στο Ubuntu Lucid και περιέχει πάνω από 350 εργαλεία για penetration testing. Ωστόσο τον Μάρτιο του 2013 αντικαταστάθηκε από το Kali Linux. Το κύριο πρόβλημα που είχε το BackTrack v1-v5 ήταν ο πονοκέφαλος με τα dependencies. Πάρα πολλά εργαλεία για pentesting ενσωματώνονταν στο BackTrack και είχαμε προβλήματα με τα dependencies.

Η λύση ήταν να ξανά κτιστή η διανομή, από την αρχή. Δημιουργώντας έτσι μια νέα διανομή που βασίζεται στο Debian. Το Kali Linux έχει προ εγκατεστημένα 300 εργαλεία .Το Kali έχει ένα νέο σύστημα Αρχείων “File system Hierarchy Standard” το οποίο μας δίνει την δυνατότητα να υποστηρίζει μια σειρά από ασύρματες συσκευές μέσα από το πρωτόκολλο plug and play.

Επίσης υπάρχει πλέον η υποστήριξη για αρχιτεκτονικές ARM όπως το Raspberry Pi και το Samsung’s ARM Chromebook. Επιπλέον έχουμε την δυνατότητα να δημιουργήσουμε το δικό μας αρχείο .iso του λειτουργικού συστήματος μέσα από τα χαρακτηριστικά του Debian. Οπως και ο προκάτοχος του είναι Open Source είναι διαθέσιμο σε 32-bit και 64-bit images για να τα χρησιμοποιήσουμε σε μηχανήματα x-86.

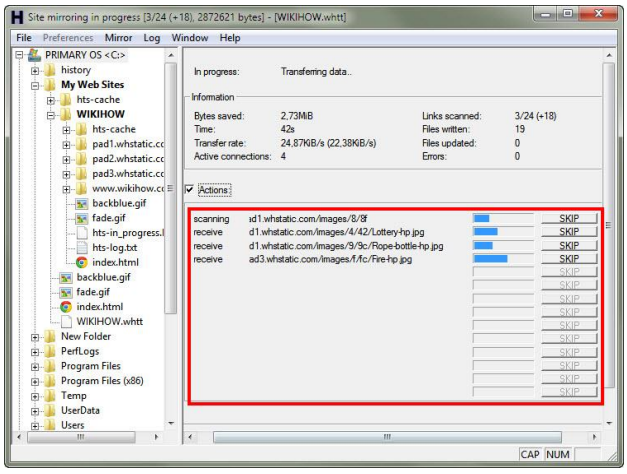
5. ΣΥΛΛΟΓΗ ΠΛΗΡΟΦΟΡΙΩΝ - INFORMATION GATHERING

Το πρώτο βήμα σε οποιαδήποτε penetration. Αυτό το σημείο είναι το λιγότερο τεχνικό αλλά είναι εξίσου σημαντικό. Όσο περισσότερες πληροφορίες μπορείτε να συλλέξετε, τόσο μεγαλύτερο ποσοστό επιτυχίας στα επόμενα στάδια.

Αρχικά, η ποσότητα των πληροφοριών που μπορούν να συγκεντρωθούν από το στόχο σας μπορεί να φαίνεται λίγο συντριπτική, αλλά με μια καλή διαδικασία τεκμηρίωσης , τη σωστή χρήση των εργαλείων , και περαιτέρω εξάσκηση θα καταλάβουμε ποσό σημαντική είναι.

HTTRACK: WEBSITE COPIER

Το HTTrack Website Copier (http://www.httrack.com/) είναι ένας δωρεάν, απλός, και πολύ καλός offline browser το οποίο μπορεί να αντιγράψει ένα διαδικτυακό τόπο τοπικά στον σκληρό μας δίσκο, τοπικά. Διατηρεί τη δομή του site που κατεβάζει, αλλά, όπως είναι φυσικό, δεν λειτουργεί σε δυναμικές ιστοσελίδες. Στις στατικές όμως τα πάει μια χαρά, έστω κι αν χρειάζονται κωδικούς εισόδου από τον χρήστη. Το περιβάλλον του είναι απλό (αν και επιδέχεται ένα σωρό ρυθμίσεις. Διατίθεται για λειτουργικά Windows (Win 8,Win 7,Vista,XP) και Linux.



ΟΙ ΟΔΗΓΙΕΣ ΤΗΣ GOOGLE

Η Google μας δίνει την δυνατότητα να χρησιμοποιήσουμε οδηγίες (directives) στην μηχανή αναζήτησης της. Οι οδηγίες αυτές είναι λέξεις- κλειδιά που μας επιτρέπουν να εξάγουμε πιο ακριβή αποτελέσματα από το ευρετήριο της Google κατά την αναζήτηση μας.

Για να χρησιμοποιήσετε σωστά μια οδηγία της Google , θα πρέπει να έχετε τρία πράγματα :

1. Το όνομα της οδηγίας που θέλετε να χρησιμοποιήσετε
2. :
3. Ο όρος που θέλετε να χρησιμοποιήσετε στην οδηγία

Παράδειγμα μιας Οδηγίας: site:apple.com steve jobs

Και κάποια αλλά Παραδείγματα Οδηγιών:

Site: .gr

Intitle: login.asp

Filetype: ppt ή pdf

Index of /

Inurl: /view/index/index.shtml

Site: .gr inurl:login.asp

THE HARVESTER: ΑΝΑΚΑΛΥΠΤΟΝΤΑΣ ΔΙΕΥΘΥΝΣΕΙΣ E-MAIL

Το Harvester (Θεριστής Διευθύνσεων) είναι ένα απλό αλλά πολύ αποτελεσματικό εργαλείο γραμμένο σε Python από τον Christian Martorella από το Edge Security. Ο Θεριστής Διευθύνσεων είναι ένα ρομπότ που σαρώνει ιστότοπους, ιστολόγια, φόρα, κτλ. αναζητώντας οτιδήποτε που μοιάζει με έγκυρη ηλεκτρονική διεύθυνση.

Αυτό αποτελεί μια μεγάλη ποσότητα ηλεκτρονικών διευθύνσεων που θα χρησιμοποιηθεί για την αποστολή ανεπιθύμητης αλληλογραφίας, ή που θα πωληθεί σε αποστολείς ανεπιθύμητης αλληλογραφίας. Το Harvester μπορεί να χρησιμοποιηθεί για την αναζήτηση στο Google , Bing , και servers PGP για e-mails , hosts, και subdomains. Επίσης μπορεί να ψάξετε το LinkedIn για τα ονόματα χρήστη. Είναι προ εγκατεστημένο στο Kali και μπορούμε να έχουμε πρόσβαση σε αυτό μέσα από την γραμμή εντολών γράφοντας την εντολή: theharvester

WHOIS

Η Whois υπηρεσία μας επιτρέπει να έχουμε πρόσβαση σε συγκεκριμένες πληροφορίες σχετικά με το στόχο μας , συμπεριλαμβανομένων των διευθύνσεων IP ή τα ονόματα κεντρικού υπολογιστή του Domain Name Systems (DNS) και τα στοιχεία επικοινωνίας που συνήθως περιέχει μια διεύθυνση και έναν αριθμό τηλεφώνου .

Η Whois υπηρεσία μας επιτρέπει να έχουμε πρόσβαση σε συγκεκριμένες πληροφορίες σχετικά με το στόχο μας.

- Διευθύνσεων IP
- Τα ονόματα κεντρικού υπολογιστή του Domain Name Systems (DNS)

- Στοιχεία επικοινωνίας συνήθως περιέχει μια διεύθυνση και έναν

WHOIS information for **syngress.com** :

```
[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SYNGRESS.COM
   Registrar: [redacted]
   Whois Server: whois.safenames.net
   Referral URL: http://www.safenames.net
   Name Server: [redacted]
   Name Server: NS2.DREAMHOST.COM
   Name Server: NS3.DREAMHOST.COM
   Status: ok
   Updated Date: 23-sep-2009
   Creation Date: 10-sep-1997
   Expiration Date: 09-sep-2015
```

NETCRAFT

Άλλο ένα εργαλείο για συλλογή πληροφοριών Netcraft (http://news.netcraft.com).

Μας παρέχει πληροφορίες σχετικά με:

- IP address
- Το Λειτουργικό σύστημα
- Τον web server
- DNS server.

Site report for www.syngress.com

Check another site

Background

Site title	*Not Present*	**Date first seen**	October 1997
Site rank	96234	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://www.syngress.com	**Last reboot**	*unknown*
Domain	syngress.com	**Netblock Owner**	New Dream Network, LLC
IP address	69.163.177.2	**Nameserver**	ns.elsevier.co.uk
IPv6 address	*Not Present*	**DNS admin**	hostmaster@elsvier.co.uk
Domain registrar	enom.com	**Reverse DNS**	ps14872.dreamhost.com
Organisation	Syngress Publishing	**Nameserver organisation**	whois.nic.uk
Top Level Domain	Commercial entities (.com)	**Hosting company**	New Dream Network
Hosting country	US	**DNS Security Extensions**	*unknown*

ΕΞΑΓΩΝΤΑΣ ΠΛΗΡΟΦΟΡΙΕΣ ΑΠΟ ΤΟΝ E-MAIL SERVERS

Οι E-mail servers μπορούν να μας παρέχουν αξιόλογες πληροφορίες. Ειδικά εάν ο στόχος μας φιλοξενεί το δικό τους e-mail server. Για να λειτουργήσει σωστά το e-mail, πρέπει να περάσει η εξωτερική κυκλοφορία μέσα από τους δρομολογητές και τα τείχη προστασίας , σε μια εσωτερική μηχανή (e-mail server), συνήθως κάπου μέσα στο προστατευόμενο δίκτυο.

METAGOOFIL

Το MetaGooFil είναι ένα εργαλείο για την εξαγωγή metadata και έχει γραφτεί από τον δημιουργό του Harvester. Τα Metadata συχνά χαρακτηρίζονται σαν “δεδομένα για τα δεδομένα”. Το MetaGooFil έρχεται προ εγκατεστημένο στο Kali και μπορούμε να το τρέξουμε είτε μέσα από το τερματικό και να γράψουμε την εντολή “metagoofil” με τις κατάλληλες επιλογές ή πηγαίνοντας στον κατάλογο που είναι εγκατεστημένο και τρέχοντας το εκτελέσιμο του, το οποίο είναι στον κατάλογο /usr/bin.

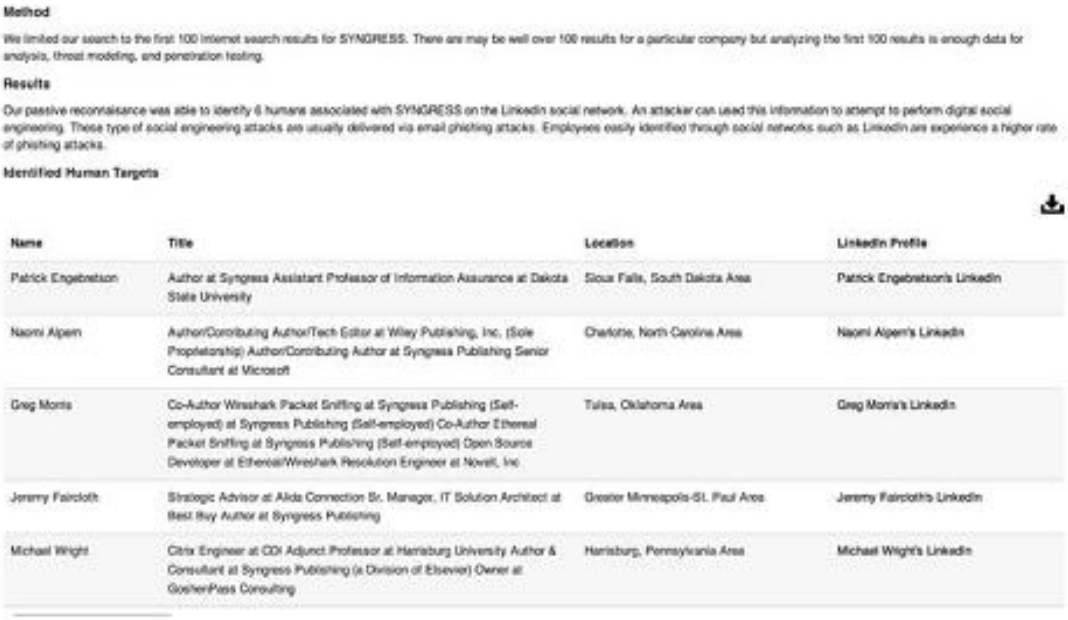
Μπορούμε να βρεθούμε εκεί μέσα από την εντολή: cd /usr/bin/metagoofil

THREAT AGENT

Έχει αναπτυχθεί από το Marcus Carey. Μπορούμε να γραφτούμε για ένα δωρεάν λογαριασμό στην διεύθυνση https://www.threatagent.com/

Το ThreatAgent πηγαίνει την διαδικασία της συλλογής πληροφοριών ένα επίπεδο υψηλοτέρα. Χρησιμοποιεί έναν αριθμό από διαφορετικούς ισότοπους, εργαλεία και τεχνικές για να «φακελώσει» τον στόχο σου. Το μόνο στοιχείο που θα χρειαστείς είναι το όνομα του στόχου σου και το domain του.

Μόλις τελειώσει την εργασία του θα μας παρουσιάσει μια αναφορά που θα περιλαμβάνει το εύρος των διευθύνσεων του IP , τις e-mail διευθύνσεις, οι θύρες που είναι ανοικτές.



Method

We limited our search to the first 100 Internet search results for SYNGRESS. There are may be well over 100 results for a particular company but analyzing the first 100 results is enough data for analysis, threat modeling, and penetration testing.

Results

Our passive reconnaissance was able to identify 6 humans associated with SYNGRESS on the LinkedIn social network. An attacker can used this information to attempt to perform digital social engineering. These type of social engineering attacks are usually delivered via email phishing attacks. Employees easily identified through social networks such as LinkedIn are experience a higher rate of phishing attacks.

Identified Human Targets

Name	Title	Location	LinkedIn Profile
Patrick Engebretson	Author at Syngress Assistant Professor of Information Assurance at Dakota State University	Sioux Falls, South Dakota Area	Patrick Engebretson's LinkedIn
Naomi Alpern	Author/Contributing Author/Tech Editor at Wiley Publishing, Inc. (Sole Proprietorship) Author/Contributing Author at Syngress Publishing Senior Consultant at Microsoft	Charlotte, North Carolina Area	Naomi Alpern's LinkedIn
Greg Morris	Co-Author Wireshark Packet Sniffing at Syngress Publishing (Self-employed) at Syngress Publishing (Self-employed) Co-Author Ethereal Packet Sniffing at Syngress Publishing (Self-employed) Open Source Developer at Ethereal/Wireshark Resolution Engineer at Novell, Inc	Tulsa, Oklahoma Area	Greg Morris's LinkedIn
Jeremy Faircloth	Strategic Advisor at Alida Connection Sr. Manager, IT Solution Architect at Best Buy Author at Syngress Publishing	Greater Minneapolis-St. Paul Area	Jeremy Faircloth's LinkedIn
Michael Wright	Citrix Engineer at CDI Adjunct Professor at Harrisburg University Author & Consultant at Syngress Publishing (a Division of Elsevier) Owner at GoshenPass Consulting	Harrisburg, Pennsylvania Area	Michael Wright's LinkedIn

6. ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ - SOCIAL ENGINEERING

Κοινωνική μηχανική είναι η διαδικασία αξιοποίησης της " ανθρώπινης " αδυναμία που είναι εγγενής σε κάθε οργανισμό. Κατά τη χρήση της κοινωνικής μηχανικής , ο στόχος του επιτιθέμενου είναι να κάνει έναν υπάλληλο να αποκαλύψει κάποιες πληροφορίες που θα πρέπει να παραμείνουν εμπιστευτικές.

Ένα Παραδείγματα: Αφήνω “τυχαία” κάπου στην εταιρεία που θέλω να ελέγξω ένα flash driver ή ένα CD που εχω τοποθετήσει έναν δούρειο ίππο ενας υπάλληλος το βρίσκει και το βάζει σε ένα υπολογιστή του δικτύου της εταιρείας είτε από περιέργεια ή για να βρει στοιχεία για τον κάτοχο και να του το επιστέψει.

Άλλος τρόπος κοινωνικής μηχανικής πολλή δημοφιλής είναι με τις πληροφορίες που έχω συλλέξει, από τα προηγούμενα βήματα, καλώ στην εταιρία και προσποιούμε ότι είμαι υπάλληλος της, και χρειάζομαι πληροφορίες για τον λογαριασμού μου.

7. SCANNING

7.1 PING

Το ping είναι μια μέθοδος για τον εντοπισμό της διαθεσιμότητας και της απόδοσης ενός απομακρυσμένου πόρου του δικτύου. Θεωρείται ότι αποτελεί το ακρωνύμιο των λέξεων "Packet Internet Groper".Αποτελεί διαδικασία με την οποία επιβεβαιώνεται η σύνδεση με έναν απομακρυσμένο υπολογιστή π.χ. μέσω Internet ή τοπικού δικτύου.

Με το ping αποστέλλεται στον απομακρυσμένο υπολογιστή ένα πακέτο δεδομένων και στη συνέχεια ο υπολογιστής που έστειλε το πακέτο, περιμένει για μία echo reply, δηλαδή την απάντηση στο πακέτο δεδομένων του ping (πολλοί το αποκαλούν και pong). Το πακέτο που αποστέλλεται με το ping ονομάζεται ICMP (Internet Control Message Protocol) echo packet. Το διάστημα μεταξύ του ping και του echo reply επιβεβαιώνει την ποιότητα της σύνδεσης και λέγεται και lag. Μια συνηθισμένη τιμή του lag πρέπει να είναι 0.02 – 0.08 δευτερόλεπτα.

Το **ping του θανάτου (POD - Ping Of Death)** είναι ένας τύπος επίθεσης σε έναν ηλεκτρονικό υπολογιστή. Η επίθεση Ping Of Death συντελείται όταν ένας ηλεκτρονικός υπολογιστής στέλνει κακοσχηματισμένα πακέτα ping σε έναν άλλο υπολογιστή με σκοπό να τον θέσει εκτός λειτουργίας.

Η επίθεση **Ping flood** ανήκει στην κατηγορία επιθέσεων άρνησης υπηρεσιών (DOS - Denial of Service) και περιλαμβάνει την συνεχή αποστολή πακέτων ping (ICMP Echo Request) από τον υπολογιστή του επιτιθέμενου προς τον υπολογιστή του αμυνόμενου. Για να επιτύχει αυτή η επίθεση θα πρέπει ο επιτιθέμενος να διαθέτει μεγαλύτερο bandwidth (εύρος ζώνης) από το θύμα.

Η επίθεση **Smurf** είναι ένα είδος επίθεσης άρνησης εξυπηρέτησης (DOS - Denial of Service) και πήρε το όνομά της από το πρώτο πρόγραμμα που την υλοποίησε Smurf. Σε μία τέτοια επίθεση, ο επιτιθέμενος χρησιμοποιεί την διεύθυνση IP broadcast διαφόρων δικτύων για να πλημμυρίσει το θύμα με πακέτα ping ICMP Echo Reply.

7.2 PORT SCANNING

Υπάρχουν συνολικά 65.536 θύρες (ports) σε κάθε υπολογιστή. Οι Θύρες μπορεί να είναι είτε για το πρωτόκολλο ελέγχου μετάδοσης (TCP) ή για το πρωτόκολλο πακέτων χρήστη (UDP) ανάλογα με την υπηρεσία που χρησιμοποιεί τη θύρα ή τη φύση της επικοινωνίας που συμβαίνουν στο Port

Port Number	Service
20	FTP data transfer
21	FTP control
22	SSH
23	Telnet
25	SMTP (e-mail)
53	DNS
80	HTTP
137–139	NetBIOS
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
3389	RDP
5800	VNC over HTTP
5900	VNC

7.3 NMAP

Το Nmap γράφτηκε από τον Gordon Lyon (γνωστός επίσης με το ψευδώνυμο Fyodor Vaskovich)είναι διαθέσιμο δωρεάν από το www.insecure.org.

Έρχεται προ εγκατεστημένο στης περισσότερες διανομές του Linux συμπεριλαμβανομένου και του Kali. Λειτουργεί ως σαρωτής ασφαλείας και χρησιμοποιείται για να ανακαλύψει κεντρικούς υπολογιστές και τις υπηρεσίες σε ένα δίκτυο υπολογιστών, δημιουργώντας έτσι ένα "χάρτη" του δικτύου. Υπάρχει διαθέσιμο και σε γραμμή εντολών και με γραφική διεπαφή.

nmap

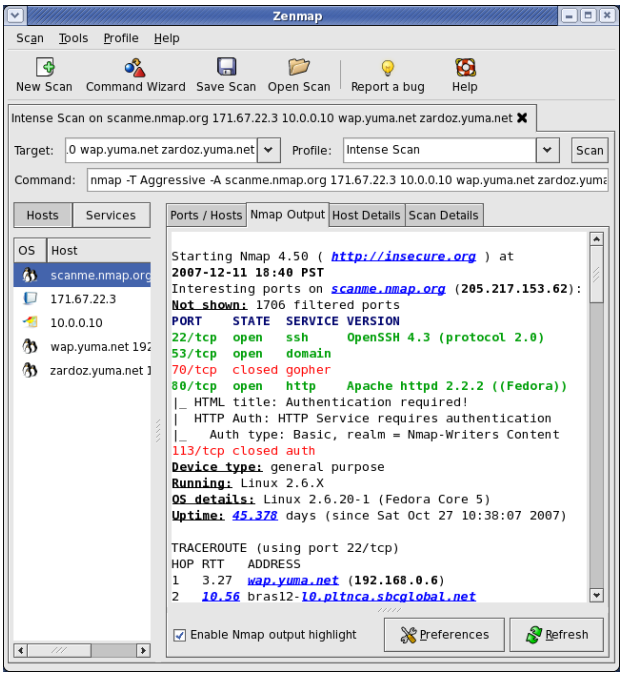
#man nmap

#nmap -p 80 192.168.2.10

#nmap -0 192.168.2.10

#nmap -p 1-200 192.168.2.10

#nmap -p 1-200 192.168.2.10 -oG nmapdata.txt

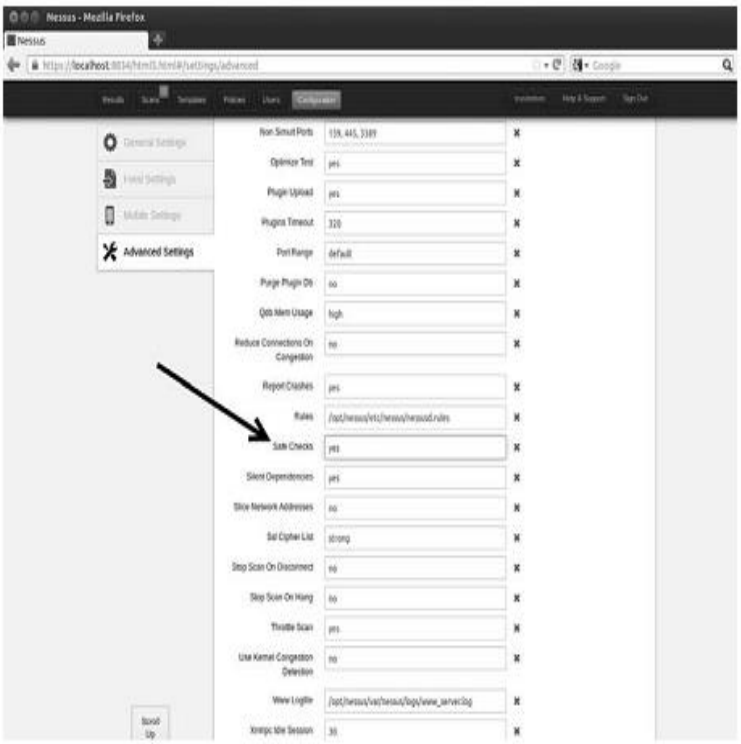


8. ΑΝΙΧΝΕΥΣΗ ΕΥΠΑΘΕΙΩΝ - VULNERABILITY SCANNING

Σαρώσει τους στόχους για τα τρωτά σημεία ευπάθειας(είναι μια αδυναμία στη διαμόρφωση του λογισμικού ή σύστημα που μπορεί συχνά να αξιοποιηθούν).

Το Nessus είναι ένα καλό εργαλείο και διατίθεται δωρεάν από την ιστοσελίδα τους στο http://www.tenable.com/products/nessus. Τρέχει σε όλα τα λειτουργικά συστήματα, συμπεριλαμβανομένων του Linux , Windows, OS X , FreeBSD και πολλά άλλα

Το Nessus λειτουργεί χρησιμοποιώντας μια αρχιτεκτονική client / server , το οποίο μας επιτρέπει να έχουμε πολλούς πελάτες πάνω στο διακοσμητή μας. https://127.0.0.1:8834 για είσοδο στο Nessus.

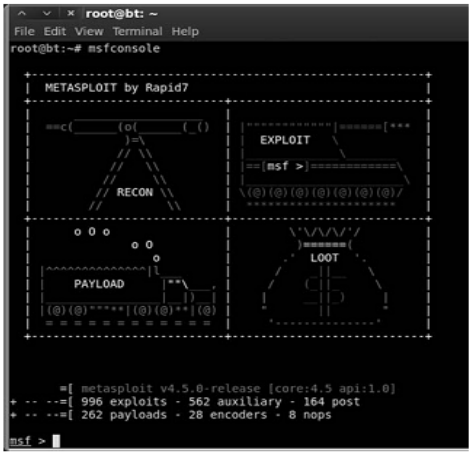


9. ΕΚΜΕΤΑΛΛΕΥΣΗ - EXPLOITATION

Σε απλούς όρους , η εκμετάλλευση είναι η διαδικασία του να αποκτήσει τον έλεγχο πάνω από ένα σύστημα.

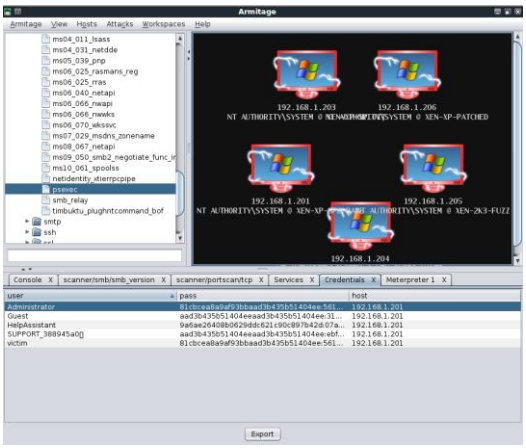
9.1 METASPLOIT

Η Διαφορά του Metasploit και ενός vulnerability scanner είναι ότι χρησιμοποιούμε ένα σαρωτή ευπάθειας (vulnerability scanner), για να ελέγξουμε εάν ένα σύστημα είναι ευάλωτο – δηλαδή μόνο για έλεγχο. Από την άλλη το Metasploit επιχειρεί να εκμεταλλευτεί πραγματικά τα συστήματα που σαρώνει. Το Metasploit μπορείτε να το κατεβάσετε δωρεάν από http://www.metasploit.com. Στο Kali το Metasploit είναι ήδη εγκατεστημένο. Υπάρχει Γραφική και μη γραφική διεπαφή διαθέσιμη για χρήση. Στην παρακάτω εικόνα βλέπουμε μια μη - γραφική διεπαφή, το σύστημα που βασίζεται σε κείμενο και ονομάζεται msfconsole



9.2 ARMITAGE

Το Armitage είναι ένα γραφικό περιβάλλον (front-end) που χρησιμοποιεί σαν βάση του το Metasploit. Το Armitage είναι διαθέσιμο δωρεάν και έρχεται εγκατεστημένο στο Backtrack. Μπορούμε να βρούμε περισσότερες πληροφορίες για το Armitage στην επίσημη σελίδα του έργου στη διεύθυνση http : // www.fastandeasyhacking.com



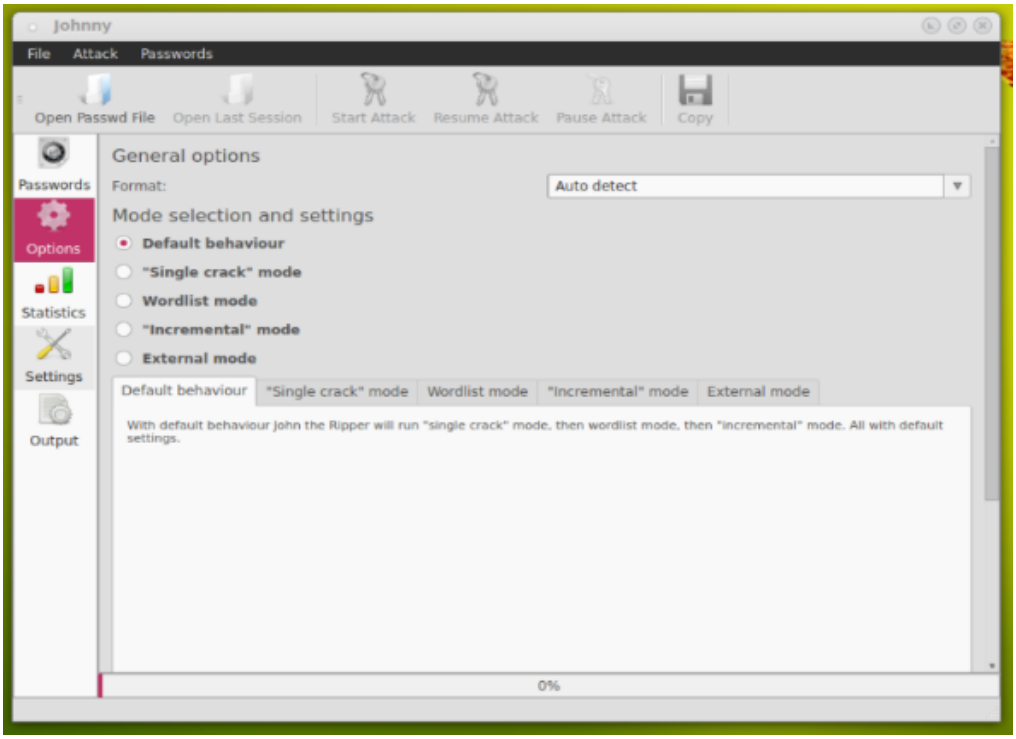
9.3 JOHN THE RIPPER

Είναι ένα πρόγραμμα για το σπάσιμο κωδίκων - password cracking. Τα πλεονεκτήματά του, Συνδυάζει πολλά πακέτα password cracking σε ένα. Μπορεί να εντοπίζει αυτόματα password που δεν είναι καθαρό κείμενο (plaintext) αλλά έχει εφαρμοστεί κάποια συνάρτηση

κατακερματισμού σε αυτά (hash). Επίσης μπορεί να τρέχει κατά πολλών γνωστών συναρτήσεων κρυπτογράφησης (DES, MD5, BlowFish, Kerberos AFS, LM hash) και με κάποια modules μπορεί να διαχειριστεί και τύπου MD4 hash passwords που βρίσκονται συνήθως σε LDAP, MySql κλπ.

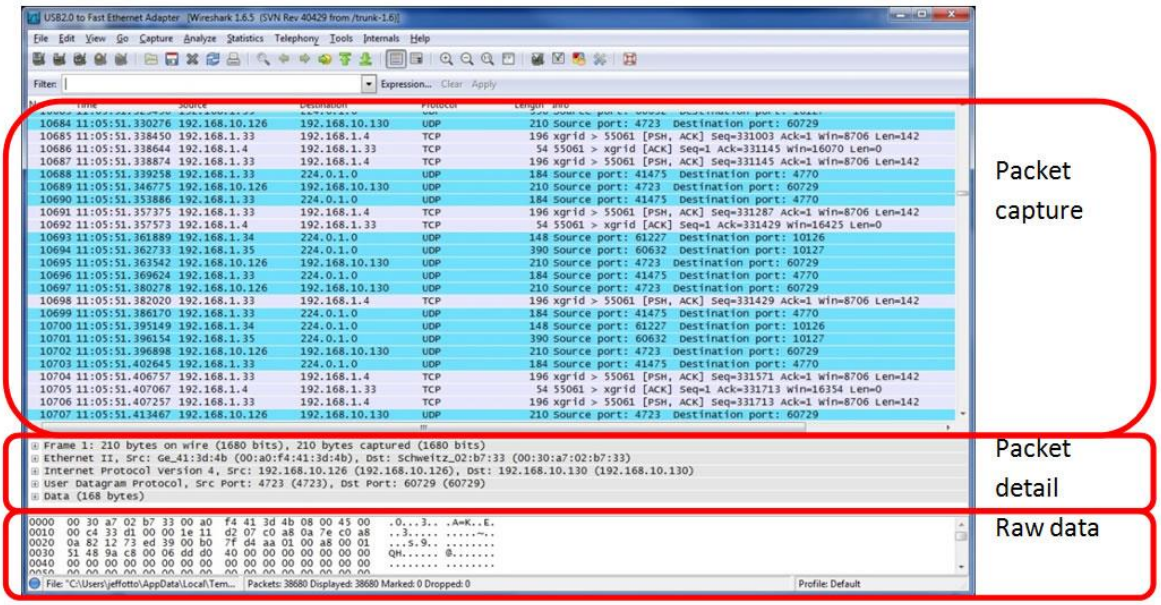
Το John the ripper μπορεί να κάνει μια επίθεση χρησιμοποιώντας ευρετήριο (wordlist) αλλά μπορεί να κάνει και bruteforce επίθεση. Όταν χρησιμοποιεί ευρετήριο, κρυπτογραφεί κάθε password ανάλογα με τον επιθυμητό τύπο κρυπτογράφησης και ψάχνει να βρει ίδιους hash codes. Το ίδιο κάνει και με τα plaintext password του bruteforce δηλαδή πρώτα παράγει σε plaintext τον κωδικό και ύστερα παράγει το hash code του.

Τέλος υπάρχει και γραφικό περιβάλλον (Johnny) για την διαχείρισή του.



9.4 WIRESHARK

Το **Wireshark** αποτελεί ένα από τα διασημότερα προγράμματα παγκοσμίως για την ανάλυση των δικτύων. Αυτό το πολύ δυνατό εργαλείο παρέχει πληροφορίες για το δίκτυο σας και των πρωτοκόλλων ανώτερου επιπέδου σχετικά με τα δεδομένα που διακινούνται σ’ αυτό.



Το Wireshark είναι ενας αναλύτης πακέτων που χρησιμοποιεί μια βιβλιοθήκη σύλληψης πακέτων στον υπολογιστή μας. Το Wireshark είναι ελεύθερο για χρήση το οποίο τρέχει σε Windows, Linux και Mac και έχει μια μεγάλη βάση χρηστών και μια καλά οργανωμένη τεκμηρίωση.

Όπως πολλά άλλα δικτυακά προγράμματα, το Wireshark χρησιμοποιεί τη δικτυακή βιβλιοθήκη pcap για την σύλληψη (ανάλυση) των πακέτων.

Η δύναμη του Wireshark πηγάζει από:
- την ευκολία εγκατάστασής του.
- την απλότητα της χρήσης του μέσω της γραφικής διεπαφής του (GUI).
- το μεγάλο αριθμό της λειτουργικότητας του.

Το Wireshark ονομαζόταν Ethereal μέχρι το 2006, όταν ο επικεφαλής προγραμματιστής, αποφάσισε την αλλαγή του ονόματός του λόγω δικαιωμάτων χρήσης που προϋπήρχαν για το όνομα Ethereal, το οποίο ήταν κατοχυρωμένο από την εταιρεία από την οποία αποφάσισε να αποχωρήσει το 2006.

10. ΕΥΡΕΣΗ ΤΗΣ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΚΑΙ ΔΙΑΤΗΡΗΣΗ ΤΗΣ ΠΡΟΣΒΑΣΗΣ - POST EXPLOITATION ANDMAINTAINING ACCESS

Σε αυτή την ενότητα θα δούμε κάποια βασικά προγράμματα που μπορούμε να χρησιμοποιήσουμε για να εκμεταλλευτούμε ένα σύστημα στο οποίο έχουμε καταφέρει να αποκτήσουμε πρόσβαση. Αυτά που θα δούμε εδώ είναι τα πιο βασικά και μπορούμε να

10.1 NETCAT: Ο ΕΛΒΕΤΙΚΟΣ ΣΟΥΓΙΑΣ ΤΩΝ ΔΙΚΤΥΩΝ

Το Netcat γράφτηκε αρχικά για να υποστηρίζει την αποστολή και λήψη τόσο στο πρωτόκολλο ελέγχου μετάδοσης (TCP) οσο και στο πρωτόκολλο πακέτων χρήστη (UDP). Το Netcat μπορεί να λειτουργήσει είτε σαν client ή σαν server. Όταν είναι σε λειτουργία πελάτη , το εργαλείο μπορεί να χρησιμοποιηθεί για να κάνει μια σύνδεση δικτύου σε άλλη υπηρεσία (συμπεριλαμβανομένης άλλη Netcat). Είναι σημαντικό να θυμόμαστε ότι Netcat μπορεί να συνδεθεί από οποιοδήποτε θύρα του υπολογιστή μας σε οποιαδήποτε θύρα στο μηχάνημα-στόχο. Ενώ όταν το Netcat εκτελείται σε κατάσταση λειτουργίας server, ενεργεί ως ακροατής όπου περιμένει να δεχθεί μια εισερχόμενη σύνδεση.

Το Netcat είναι απίστευτα απλό και απίστευτα ευέλικτο εργαλείο που επιτρέπει την επικοινωνία και την κυκλοφορία του δικτύου να ρέει από το ένα μηχάνημα στο άλλο.

Ευελιξία του Netcat το καθιστά μια εξαιρετική επιλογή

- Για μια κερκόπορτα (backdoor)
- Μπορεί να χρησιμοποιηθεί για τη μεταφορά αρχείων μεταξύ μηχανημάτων
- Να κάνει port scans
- Να χρησιμεύσει ως ένα ελαφρύ εργαλείο επικοινωνίας instant messenger/chat
- και μπορεί να λειτουργήσει ως ένα απλό web server !

10.2 ΤΟ ΞΑΔΕΡΦΑΚΙ ΤΟΥ NETCAT, ΤΟ CRYPTCA

Πρώτα από όλα , είναι σημαντικό να καταλάβουμε ότι όλη η κίνηση που διέρχεται μεταξύ ενός πελάτη και του διακομιστή στο Netcat γίνεται σε μορφή απλού κειμένου. Αυτό σημαίνει ότι οποιοσδήποτε είναι σε θέση να δείτε και να παρακολουθεί όλες τις πληροφορίες που αποστέλλονται μεταξύ των μηχανών. Το Cryptcat χρησιμοποιεί συμμετρική κρυπτογράφηση Twofish για να κρατήσει την κίνηση μεταξύ του πελάτη και του διακομιστή εμπιστευτική .

Μια σημαντική σημείωση για Cryptcat ,

θα πρέπει πάντα να αλλάξετε το προεπιλεγμένο κλειδί .Το προεπιλεγμένο κλειδί είναι Metallica και μπορεί να αλλάξει με τη χρήση του "ek"

Για να δημιουργήσουμε ένα κρυπτογραφημένο κανάλι μεταξύ δυο μηχανήματων χρησιμοποιώντας το Cryptcat, μπορούμε να χρησιμοποιήσουμε τις παρακάτω εντολές:

(1) Start the server:

cryptcat el ep 5757

(2) Start the client:

cryptcat 192.168.18.132 5757

10.3 ROOTKITS

Το όνομα rootkit πιθανολογείτε ότι προέρχεται από την ένωση των λέξεων "root", ο διαχειριστής συστήματος και "kit" συλλογή εργαλείων. Τα Rootkits μπορούν να χρησιμοποιηθούν για να κρύψει τα αρχεία από τους χρήστες και ακόμη και το ίδιο το λειτουργικό σύστημα.

Επειδή τα rootkits είναι τόσο αποτελεσματικά στο να κρύβουν αρχεία , συχνά είναι επιτυχής στο να αποφύγει ακόμη και τον έλεγχο των προγραμμάτων antivirus. Πολλοί rootkits είναι σε θέση να αποφύγουν τον εντοπισμό επειδή λειτουργούν σε πολύ χαμηλότερο επίπεδο από το ίδιο το λειτουργικό σύστημα , στο εσωτερικό του πυρήνα .

Μπορούν να χρησιμοποιηθούν για την Προσθήκη Προνομίων σε χρήστες, την Καταγραφή Πληκτρολόγησης την Εγκατάσταση backdoors Και για άλλες εργασίες.

Είναι σημαντικό να επισημάνουμε ότι το rootkit δεν είναι ένα exploit. Τα Rootkits είναι κάτι που έχει ανεβάσει στο σύστημα μετά την αξιοποιήσει (exploit) του συστήματος. Τα rootkits συνήθως χρησιμοποιείται για να κρύψει τα αρχεία ή προγράμματα και να διατηρήσουν μια κερκόπορτα (backdoor) πρόσβαση .

11 ΣΥΜΠΕΡΑΣΜΑΤΑ

Συνοψίζοντας στην παραπάνω εργασία προσπαθήσαμε να κάνουμε μια σύντομη άλλα πλήρη αναφορά στο Penetration Testing να δούμε τις μεθόδους, τις τεχνικής και τα εργαλεία που χρησιμοποιούμε κατά τον Έλεγχο της Ασφάλειας σε ένα σύστημα.

Καθώς επίσης και τον τρόπο που γράφουμε μια τεχνική αναφορά για να αναφέρουμε τα αποτελέσματα του τεστ που πραγματοποιήσαμε πάνω σε ένα πληροφοριακά σύστημα. Αυτό που προσπαθήσαμε ήταν να κάνουμε μια περιγραφή τόσο της διαδικασίας όσο και των τεχνικών αλλά και τον εργαλείων με ένα τρόπο που να είναι εύκολος στην κατανοητή χωρίς πολλές τεχνικές λεπτομέρειες και συνοπτικός σαν μια πρώτη επαφή με την διαδικασία και τα εργαλεία που χρησιμοποιούμε.

Στόχος της εργασίας ήταν να κάνουμε μια σύντομη άλλα περιεκτική αναφορά σε όλα τα στάδια της διαδικασίας του έλεγχού της ασφάλειας σε ένα πληροφοριακό σύστημα. Κάθε κεφάλαιο για να είναι πλήρης είναι από μονό του μια καινούργια εργασία για να μπορέσει να καλυφθεί σε βάθος και σε ένα ικανοποιητικό βαθμό.

Καθώς το αντικείμενο του ελεγου ειδικά σε θέματα ασφάλειας πληροφοριακών συστημάτων α λλάζει πάρα πολλήγρήγορα γίνεται κατανοητό ότι μονό η συνεχείς ενασχόληση με το αντικείμενο είναι σε θέση
να δημιουργήσουν τις κατάλληλες δεξιότητες να εκτελούμε αποδοτικότερα τις τεχνικές που αν αφερθήκαν άλλα και να κάνουμε καλύτερη χρήση των εργαλείων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Patrick Engebretson -The basics of hacking and penetration testing ethical hacking and penetration testing made easy

Joseph Muniz, Aamir Lakhani - Web Penetration Testing with Kali Linux

Georgia Weidman –Penetration testing A Hands-On Introduction to Hacking

Baloch, Rafay - Ethical Hacking and Penetration Testing Guide